This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A method of propagating rights management ~~(RM)~~ protection to an email and to an attachment of the email, the attachment comprising an ~~RM~~ rights-management-protectable document, the method comprising:

authoring the email with the ~~RM~~ rights-management-protectable attachment;

generating a content key ~~(KD)~~;

generating a bind ~~ID~~ identifier;

firstly applying ~~RM~~ rights management protection to the ~~RM~~ rights-management-protectable attachment of the email based on the generated content key ~~(KD)~~ and the generated bind ~~ID~~ identifier;

attaching the ~~RM~~ rights-management-protectable attachment to the email;

secondly applying ~~RM~~ rights management protection to the combined email ~~with the~~ and attached ~~RM~~ rights-management-protectable attachment based on the generated content key ~~(KD)~~ and the generated bind ~~ID~~ identifier;

wherein the ~~RM~~ rights-management-protected email and the ~~RM~~ rights-management-protectable attachment thereof share the generated content key ~~(KD)~~ and the generated bind~~ID~~ identifier such that a license obtained for the ~~RM~~ rights-management-protected email and having therein the generated bind ~~ID~~ identifier and the generated content key ~~(KD)~~ can be applied to render the ~~RM~~ rights-management-protected email and also the ~~RM~~ rights-management-protectable attachment thereof.

2. (Currently Amended) The method of claim 1 further comprising:

providing content key ~~(KD)~~ to an ~~RM~~ rights management server so that all requests for a license corresponding to ~~the~~ an item are directed to such ~~RM~~ rights management server; and

generating rights data including the protected content key ~~(KD)~~ and the generated bind ~~ID~~ identifier and setting forth each entity that has rights with respect to the ~~RM~~ rights-management-protected email and the ~~RM~~ rights-management-

protectable attachment thereof and for each such entity a description of such rights; and

wherein applying ~~RM~~ rights management protection to each item comprises:

encrypting the item with content key ~~(KD)~~ to form ~~(KD(item))~~ a content-key-encrypted item; and

attaching the rights data to the corresponding ~~(KD(item))~~ content-key-encrypted item to form a package containing the item in an ~~RM~~ rights-management-protected form, whereby the ~~signed~~ rights data from the package for any item may be employed to obtain the license for the ~~RM~~ rights-management-protected email and the ~~RM~~ rights-management-protectable attachment thereof, such license thus including the bind ~~ID~~ identifier of the ~~signed~~ rights data and being bound to the ~~RM~~ rights-management-protected email and the ~~RM~~ rights-management-protectable attachment thereby.

3. (Original) The method of claim 2 further comprising submitting the generated rights data for signing and receiving signed rights data based thereon, whereby the signed rights data is tamper-resistant in that any changes to the signed rights data will cause the signature to fail to verify, and wherein attaching the rights data comprises attaching the signed rights data.

4. (Currently Amended) The method of claim 3 wherein submitting the rights data for signing comprises submitting the rights data to the ~~RM~~ rights management server for signing.

5. (Currently Amended) The method of claim 2 wherein protecting content key ~~(KD)~~ comprises encrypting content key ~~(KD)~~ with a public key of the ~~RM~~ rights management server to result in ~~(PU-RM(KD))~~ a rights-management-public-key-encrypted content key such that only the ~~RM~~ rights management server with a corresponding ~~private key (PR-RM)~~ rights management private key can decrypt ~~(PU-RM(KD))~~ the rights-management-public-key-encrypted content key to reveal the content key ~~(KD)~~.

6. (Currently Amended) The method of claim 2 wherein attaching the rights data comprises concatenating the signed rights data with the corresponding ~~(KD(item))~~ content-key-encrypted item to form a package containing the item in an ~~RM~~ rights-management-protected form.

7. (Currently Amended) ~~An email having an attachment~~ A computer readable storage medium having stored thereon an email and an associated attachment, the email and the attachment being rights management ~~(RM)~~ protected, the attachment of the email being ~~RM~~ rights-management-protected based on a particular content key ~~(KD)~~ and a particular bind ~~ID~~ identifier, the email with the ~~RM~~ rights-management-protected attachment itself being ~~RM~~ rights-management-protected based on the particular content key ~~(KD)~~ and the particular bind ~~ID~~ identifier, wherein the ~~RM~~ rights-management-protected email with the ~~RM~~ rights-management-protected attachment therein share the particular content key ~~(KD)~~ and the particular bind ~~ID~~ identifier such that a license obtained for the ~~RM~~ rights-management-protected email and having therein the generated bind ~~ID~~ identifier and the generated content key ~~(KD)~~ can be applied to render the ~~RM~~ rights-management-protected email and also the ~~RM~~ rights-management-protected attachment therein.

8. (Currently Amended) The ~~email~~ medium of claim ~~1~~ 7 wherein the ~~RM~~ rights management protection for each item comprises the item being encrypted with content key ~~(KD)~~ to form ~~(KD(item))~~ a content-key-encrypted item and having attached thereto common rights data to form a package containing the item in an ~~RM~~ rights-management-protected form, the common rights data including the particular bind ~~ID~~ identifier and the particular content key ~~(KD)~~ protected to an ~~RM~~ rights management server so that all requests for a license corresponding to the item are directed to such ~~RM~~ rights management server, and setting forth each entity that has rights with respect to the ~~RM~~ rights-management-protected email and the ~~RM~~ rights-management-protected attachment thereof and for each such entity a description of such rights, whereby the rights data from the package for any item may be employed to obtain the license for the ~~RM~~ rights-management-protected email and the ~~RM~~ rights-management-protected attachment therein, such license thus including the bind ~~ID~~

identifier of the signed rights data and being bound to the ~~RM~~ rights-management-protected email and the ~~RM~~ rights-management-protected attachment thereby.

9. (Currently Amended) The ~~email~~ medium of claim 8 wherein the common rights data comprises rights data submitted for signing and received as signed rights data based thereon, whereby the signed rights data is tamper-resistant in that any changes to the signed rights data will cause the signature to fail to verify.

10. (Currently Amended) The ~~email~~ medium of claim 9 wherein the rights data is submitted to the ~~RM~~ rights management server for signing.

11. (Currently Amended) The ~~email~~ medium of claim 8 wherein the content key ~~(KD)~~ protected comprises the content key ~~(KD)~~ encrypted with a public key of the ~~RM~~ rights management server to result in ~~(PU-RM(KD))~~ a rights-management-public-key-encrypted content key such that only the ~~RM~~ rights management server with a corresponding ~~private key (PR-RM)~~ rights management private key can decrypt ~~(PU-RM(KD))~~ the rights-management-public-key-encrypted content key to reveal the content key ~~(KD)~~.

12. (Currently Amended) The ~~email~~ medium of claim 8 wherein the rights data is concatenated with the corresponding ~~(KD(item))~~ content-key-encrypted item to form a package containing the item in an ~~RM~~ rights-management-protected form.

13. (Currently Amended) A computer-readable storage medium having stored thereon computer-executable instructions for performing a method of propagating rights management ~~(RM)~~ protection to an email and to an attachment of the email, the attachment comprising an ~~RM~~ rights-management-protectable document, the method comprising:

authoring the email with the ~~RM~~ rights-management-protectable attachment;

generating a content key ~~(KD)~~;

generating a bind ~~ID~~ identifier;

firstly applying ~~RM~~ rights management protection to the ~~RM~~ rights-management-protectable attachment of the email based on the generated content key ~~(KD)~~ and the generated bind ~~ID~~ identifier;

attaching the ~~RM~~ rights-management-protectable attachment to the email;

secondly applying ~~RM~~ rights management protection to the combined email ~~with the~~ and attached ~~RM~~ rights-management-protectable attachment based on the generated content key ~~(KD)~~ and the generated bind ~~ID~~ identifier;

wherein the ~~RM~~ rights-management-protected email and the ~~RM~~ rights-management-protectable attachment thereof share the generated content key ~~(KD)~~ and the generated bind ~~ID~~ identifier such that a license obtained for the ~~RM~~ rights-management-protected email and having therein the generated bind ~~ID~~ identifier and the generated content key ~~(KD)~~ can be applied to render the ~~RM~~ rights-management-protected email and also the ~~RM~~ rights-management-protectable attachment thereof.

14. (Currently Amended) The medium of claim 13 wherein the method further comprises:

protecting content key ~~(KD)~~ to an ~~RM~~ rights management server so that all requests for a license corresponding to ~~the~~ an item are directed to such ~~RM~~ rights management server; and

generating rights data including the protected content key ~~(KD)~~ and the generated bind ~~ID~~ identifier and setting forth each entity that has rights with respect to the ~~RM~~ rights-management-protected email and the ~~RM~~ rights-management-protectable attachment thereof and for each such entity a description of such rights; and

wherein applying ~~RM~~ rights management protection to each item comprises:

encrypting the item with content key ~~(KD)~~ to form ~~(KD(item))~~ a content-key-encrypted item; and

attaching the rights data to the corresponding ~~(KD(item))~~ content-key-encrypted item to form a package containing the item in an ~~RM~~ rights-management-protected form, whereby the ~~signed~~ rights data from the package for any item may be employed to obtain the license for the ~~RM~~ rights-

management-protected email and the ~~RM~~ rights-management-protectable attachment thereof, such license thus including the bind ~~ID~~ identifier of the ~~signed~~ rights data and being bound to the ~~RM~~ rights-management-protected email and the ~~RM~~ rights-management-protectable attachment thereby.

15. (Original) The medium of claim 14 wherein the method further comprises submitting the generated rights data for signing and receiving signed rights data based thereon, whereby the signed rights data is tamper-resistant in that any changes to the signed rights data will cause the signature to fail to verify, and wherein attaching the rights data comprises attaching the signed rights data.

16. (Currently Amended) The medium of claim 15 wherein submitting the rights data for signing comprises submitting the rights data to the ~~RM~~ rights management server for signing.

17. (Currently Amended) The medium of claim 14 wherein protecting content key ~~(KD)~~ comprises encrypting content key ~~(KD)~~ with a public key of the ~~RM~~ rights management server to result in ~~(PU-RM(KD))~~ a rights-management-public-key-encrypted content key such that only the ~~RM~~ rights management server with a corresponding ~~private key (PR-RM)~~ rights management private key can decrypt ~~(PU-RM(KD))~~ the rights-management-public-key-encrypted content key to reveal content key ~~(KD)~~.

18. (Currently Amended) The medium of claim 14 wherein attaching the rights data comprises concatenating the signed rights data with the corresponding ~~(KD(item))~~ content-key-encrypted item to form a package containing the item in an ~~RM~~ rights-management-protected form.

19. (Currently Amended) A computer-readable storage medium having stored thereon a data structure comprising an email having an attachment, the email and the attachment being rights management ~~(RM)~~ protected, the attachment of the email being ~~RM~~ rights-management-protected based on a particular content key ~~(KD)~~ and a particular bind ~~ID~~

identifier, the email with the ~~RM~~ rights-management-protected attachment itself being ~~RM~~ rights-management-protected based on the particular content key ~~(KD)~~ and the particular bind ~~ID~~ identifier, wherein the ~~RM~~ rights-management-protected email with the ~~RM~~ rights-management-protected attachment therein share the particular content key ~~(KD)~~ and the particular bind ~~ID~~ identifier such that a license obtained for the ~~RM~~ rights-management-protected email and having therein the generated bind ~~ID~~ identifier and the generated content key ~~(KD)~~ can be applied to render the ~~RM~~ rights-management-protected email and also the ~~RM~~ rights-management-protected attachment therein.

20. (Currently Amended) The medium of claim 19 wherein the ~~RM~~ rights management protection for each item comprises the item being encrypted with content key ~~(KD)~~ to form ~~(KD(item))~~ a content-key-encrypted item and having attached thereto common rights data to form a package containing the item in an ~~RM~~ rights-management-protected form, the common rights data including the particular bind ~~ID~~ identifier and the particular content key ~~(KD)~~ protected to an ~~RM~~ rights management server so that all requests for a license corresponding to the item are directed to such ~~RM~~ rights management server, and setting forth each entity that has rights with respect to the ~~RM~~ rights-management-protected email and the ~~RM~~ rights-management-protected attachment thereof and for each such entity a description of such rights, whereby the rights data from the package for any item may be employed to obtain the license for the ~~RM~~ rights-management-protected email and the ~~RM~~ rights-management-protected attachment therein, such license thus including the bind ~~ID~~ identifier of the signed rights data and being bound to the ~~RM~~ rights-management-protected email and the ~~RM~~ rights-management-protected attachment thereby.

21. (Original) The medium of claim 20 wherein the common rights data comprises rights data submitted for signing and received as signed rights data based thereon, whereby the signed rights data is tamper-resistant in that any 20 changes to the signed rights data will cause the signature to fail to verify.

22. (Currently Amended) The medium of claim 21 wherein the rights data is submitted to the ~~RM~~ rights management server for signing.

23. (Currently Amended) The medium of claim 20 wherein content key ~~(KD)~~ protected comprises content key ~~(KD)~~ encrypted with a public key of the ~~RM~~ rights management server to result in ~~(PU-RM(KD))~~ a rights-management-public-key-encrypted content key such that only the ~~RM~~ rights management server with a corresponding ~~private key (PR-RM)~~ rights management private key can decrypt ~~(PU-RM(KD))~~ the rights-management-public-key-encrypted content key to reveal content key ~~(KD)~~.

24. (Currently Amended) The medium of claim 20 wherein the rights data is concatenated with the corresponding ~~(KD(item))~~ content-key-encrypted item to form a package containing the item in an ~~RM~~ rights-management-protected form.